PERMISSIONS GRANTED DURING SETUP
(AFTER PTSEC CHANGES)

PERMISSIONS ON OBJECTS IN THE EXCHANGE CONFIGURATION TREE:

Microsoft Exchange container

cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During ForestPrep phase					
Authenticated Users				ACTRL_DS_LIST | ACTRL_DS_READ_PROP	
*Designated admin account				DS_AM_FULL_CONTROL	
During server install					
Exchange Domain Servers				STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST	
During ADC setup					
Exchange Services				DS_AM_FULL_CONTROL	

* Set via call into Delegation Wizard code

ADC Connection Agreement container

cn=Active Directory Connections,cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During server install					
Exchange Domain Servers				DS_AM_FULL_CONTROL	

Organization container

cn=<organization>,cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property/Applies To**
During ForestPrep phase					
Authenticated Users	☑			ACTRL_DS_LIST_OBJECT | ACTRL_DS_READ_PROP	
*Designated admin account		☑	☑	Send-As	
*Designated admin account		☑	☑	Receive-As	
During Server install					
“Enterprise Admins”		☑	☑	Send-As	
“Enterprise Admins”		☑	☑	Receive-As	
“Domain Admins” of root domain		☑	☑	Send-As	
“Domain Admins” of root domain		☑	☑	Receive-As	
Everyone	☑		☑	ms-Exch-Create-Top-Level-Public-Folder	
Everyone	☑		☑	ms-Exch-Create-Public-Folder	
Everyone	☑		☑	ms-Exch-Store-Create-Named-Properties	
Everyone	☑		☑	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST | ACTRL_LIST_OBJECT	Applies to object class: msExchPrivateMDB
Everyone	☑		☑	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST | ACTRL_LIST_OBJECT	Applies to object class: msExchPublicMDB
Everyone	☑		☑	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST | ACTRL_LIST_OBJECT	Applies to object class: mTA
Exchange Domain Servers	☑		☑	DS_AM_CONTROL_ACCESS (i.e, all extended rights)	
Exchange Domain Servers	☑		☑	ACTRL_DS_CREATE_CHILD	
Exchange Domain Servers	☑		☑	ACTRL_DS_WRITE_PROP	Public-Information (property set)
Exchange Domain Servers	☑		☑	ACTRL_DS_WRITE_PROP	Personal-Information (property set)
Exchange Domain Servers	☑		☑	DS_AM_FULL_CONTROL	Applies to object class: siteAddressing
When enabling an SRS (ACE is removed when SRS is disabled)					
MACHINE$	☑		☑	ACTRL_DS_LIST_OBJECT | ACTRL_DS_CREATE_CHILD| ACTRL_DS_DELETE_CHILD	

* Set via call into Delegation Wizard code

Address Lists container

cn=Address Lists Container,cn=<organization>,cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
Authenticated Users	□		□	ACTRL_DS_LIST	

Addressing container

cn=Addressing,cn=<organization>,cn=Microsoft Exchange,cn=Services,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
Authenticated Users	☐		☐	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST	

Recipient Update Services container

cn=Recipient Update Services,cn=Address Lists Container,cn=<organization>,cn=Microsoft Exchange,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
Exchange Domain Servers	☐		☐	DS_AM_FULL_CONTROL	

Administrative Group

cn=<admin group>,cn=Administrative Groups,cn=<organization>,cn=Microsoft Exchange,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install ***(set on attribute msExchPFDefaultAdminACL)***					
Authenticated Users	☐		☐	ms-Exch-Create-Public-Folder	

Default TLH

cn=Public Folders,cn=All Folder Hierarchies,cn=<admin group>,cn=Administrative Groups,cn=<organization>,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install ***(set on attribute msExchPFDefaultAdminACL)***					
Authenticated Users	☐		☐	ms-Exch-Create-Public-Folder	

CA container

cn=CA,cn=Advanced Security,cn=<admin group>,cn=Administrative Groups,cn=<organization>,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During KMS install					
MACHINE$	☐		☐	DS_AM_FULL_CONTROL	
Authenticated Users	☐		☐	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP	

Connections Container

cn=Connections,cn=<routing group>,cn=Routing Groups,cn=<admin group>,cn=Administrative Groups,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
Exchange Domain	☐		☐	DS_AM_FULL_CONTROL	

Servers					

Server object

cn=<server>,cn=Servers,cn=<admin group>,cn=Administrative Groups,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install, if the server is NOT a cluster VM					
MACHINE$	☐		☐	DS_AM_FULL_CONTROL	
During Server install, if the server IS a cluster VM					
Exchange Domain Servers	☐		☐	DS_AM_FULL_CONTROL	

Protocols Container

cn=Protocols,cn=<server>,cn=Servers,cn=<admin group>,cn=Administrative Groups,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
Everyone	☐		☐	ACTRL_DS_LIST	
Everyone	☐		☐	ms-Exch-Read-Metabase-Properties	

System Attendant object

cn=Microsoft System Attendant,cn=<server>,cn=Servers,cn=<admin group>,cn=Administrative Groups,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install ***(set on attribute msExchMailboxSecurityDescriptor)***					
LocalSystem				READ_CONTROL | fsdspermUserSendAs | fsdspermUserMailboxOwner	
Exchange Domain Servers				READ_CONTROL | fsdspermUserSendAs | fsdspermUserMailboxOwner	
5.5 Service Account (if given)				READ_CONTROL | fsdspermUserSendAs | fsdspermUserMailboxOwner	

MTA object

cn=Microsoft MTA,cn=<server>,cn=Servers,cn=<admin group>,cn=Administrative Groups,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During Server install					
5.5 Service Account (if given)				Send-As	
5.5 Service Account (if given)				Read-As	

PERMISSIONS ON OTHER OBJECTS IN THE CONFIGURATION TREE:

Deleted Items container

cn=Deleted Items,cn=Configuration,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During ForestPrep phase					
*Designated admin account	☐		☐	STANDARD_RIGHTS_READ | ACTRL_DS_LIST | ACTRL_DS_READ_PROP | ACTRL_DS_LIST_OBJECT | WRITE_OWNER | WRITE_DAC	
During Server install					
Exchange Domain Servers	☐		☐	ACTRL_DS_LIST	

* Set via call into Delegation Wizard code

Active Directory Connector object

cn=Active Directory Connector,cn=Exchange Settings,cn=<server>,cn=Servers,cn=<site>,cn=sites,cn=Configuration,...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During ADC setup					
Exchange Services	☐		☐	DS_AM_FULL_CONTROL	
Authenticated Users	☐		☐	STANDARD_RIGHTS_READ | ACTRL_DS_READ_PROP | ACTRL_DS_LIST	

MachineEnrollmentAgent object

cn=MachineEnrollmentAgent,cn=Certificate Templates,cn=Public Key Services,cn=Services,cn=Configuration,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During KMS install					
MACHINE$	☐		☐	DS_AM_FULL_CONTROL	

ExchangeUser object

cn=ExchangeUser,cn=Certificate Templates,cn=Public Key Services,cn=Services,cn=Configuration,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During KMS install					
MACHINE$	☐		☐	READ_CONTROL | ACTRL_DS_LIST | ACTRL_DS_READ_PROP	
MACHINE$	☐		☐	Enroll	

ExchangeUserSignature object

cn=ExchangeUserSignature,cn=Certificate Templates,cn=Public Key Services,cn=Services,cn=Configuration,cn=...					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During KMS install					
MACHINE$	☐		☐	READ_CONTROL |	

				ACTRL_DS_LIST | ACTRL_DS_READ_PROP	
MACHINE$	□		□	Enroll	

PERMISSIONS ON OBJECTS IN THE DOMAIN NAMING CONTEXT:

Domain container

dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During DomainPrep phase					
Exchange Enterprise Servers	☑		☑	ACTRL_DS_WRITE_PROP	Public-Information (property set)
Exchange Enterprise Servers	☑		☑	ACTRL_DS_WRITE_PROP	Personal-Information (property set)
Exchange Enterprise Servers	☑		☑	ACTRL_DS_WRITE_PROP	groupType
Exchange Enterprise Servers	☑		☑	DS-Replication-Manage-Topology	

Domain proxy container

cn=Microsoft Exchange System Objects,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During DomainPrep phase					
Exchange Enterprise Servers	☑			DS_AM_FULL_CONTROL	
Exchange Domain Servers	☑		☑	DS_AM_FULL_CONTROL	

“Exchange Enterprise Servers” group

cn=Exchange Enterprise Servers,cn=Users,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During DomainPrep phase					
All org-level full Exchange admins	☑			DS_AM_FULL_CONTROL	
Exchange Enterprise Servers	☑			DS_AM_FULL_CONTROL	

“Exchange Domain Servers” group

cn=Exchange Domain Servers,cn=Users,dc=<domain>					
Account	**Allow**	**Deny**	**Inherit**	**Right**	**On Property**
During DomainPrep phase					
All org-level full Exchange admins	☑			DS_AM_FULL_CONTROL	
Exchange Enterprise Servers	☑			DS_AM_FULL_CONTROL	